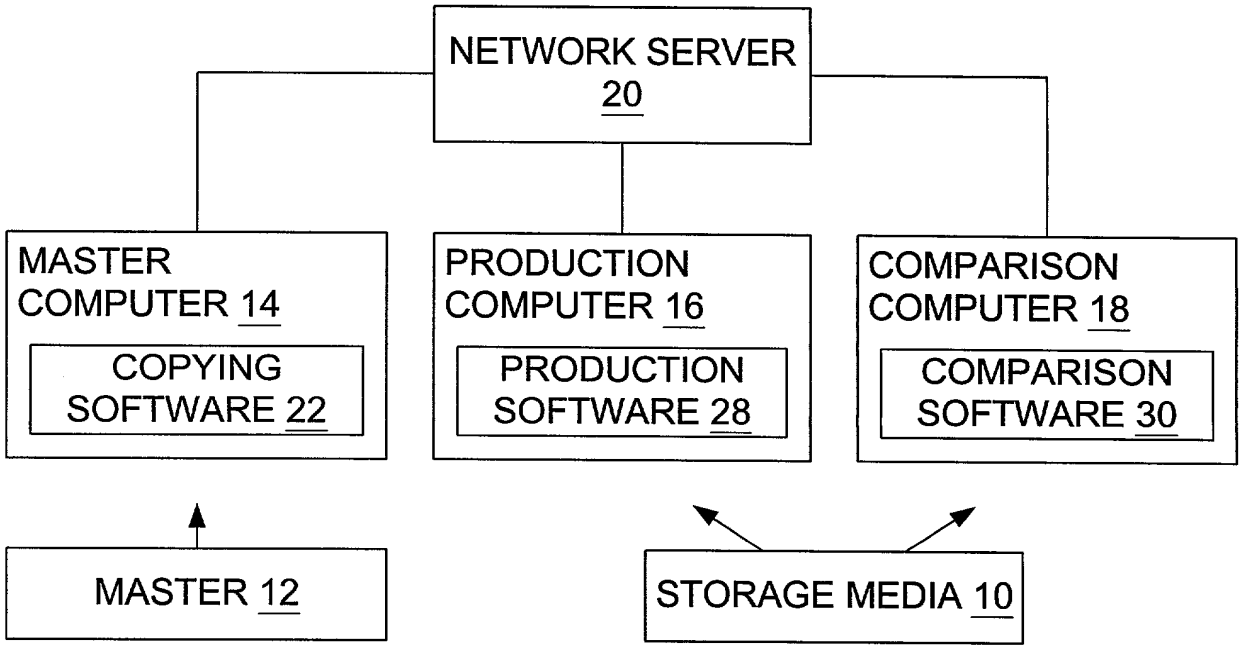

FIG. 1

MASTER IMAGE 24
BOOT INFO. [LOGICAL BLOCK 0]
DEAD SPACE [LOGICAL BLOCKS 1-31] - PART ID. BYTE COUNT -PART ID. -ENCRYPTED SECURITY ID. BYTE COUNT -ENCRYPTED SECURITY ID.
FAT(s) [LOGICAL BLOCK 32]
PARTITION INFO.
DIRECTORY ENTRIES
DATA FILES

FIG. 3

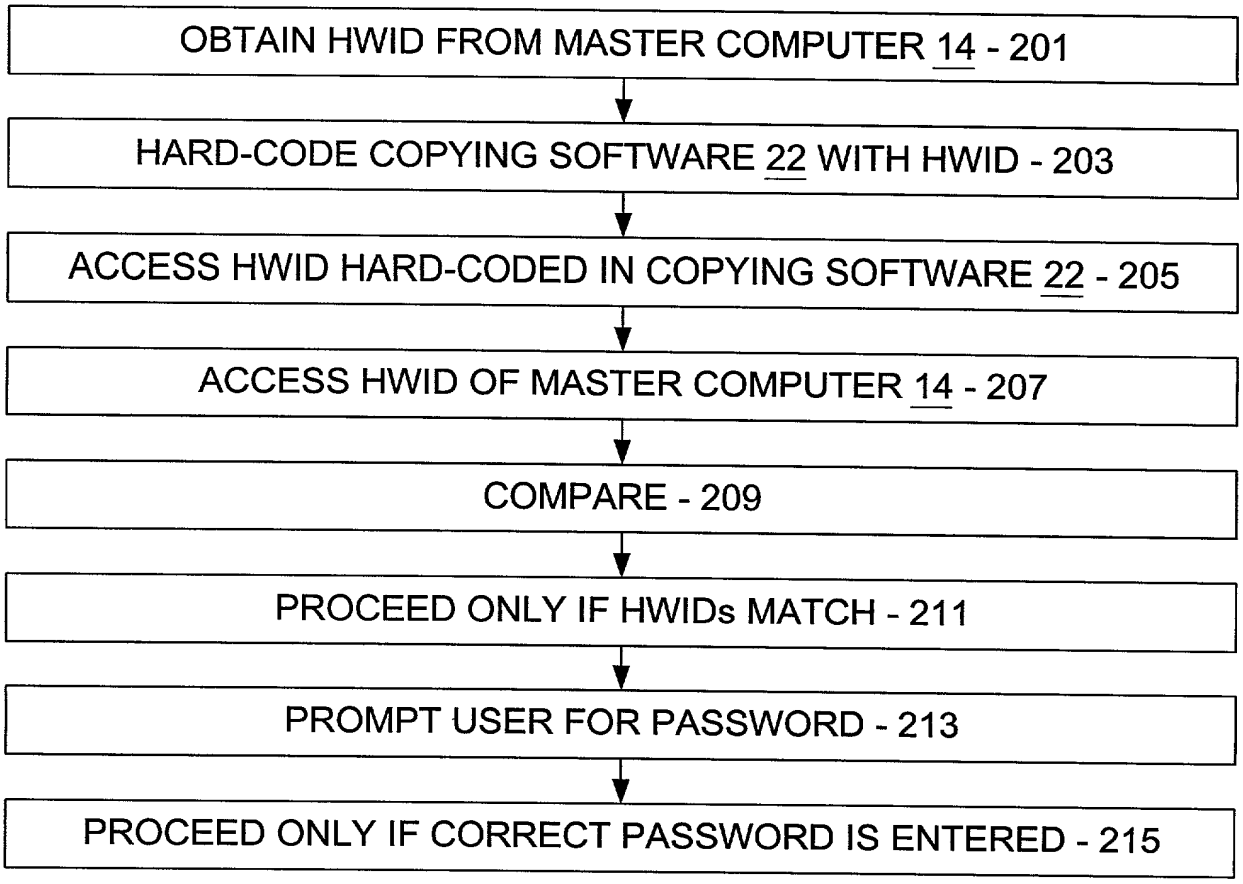

FIG. 2

IMAGE DATA FILE 26		
IMAGE FILE NAME	PART ID.	CHECKSUM
IMAGE027.MST	0E123	2134321219
IMAGE028.MST	2133D	6753976543
IMAGE029.MST	2A232	7225433654

FIG. 5

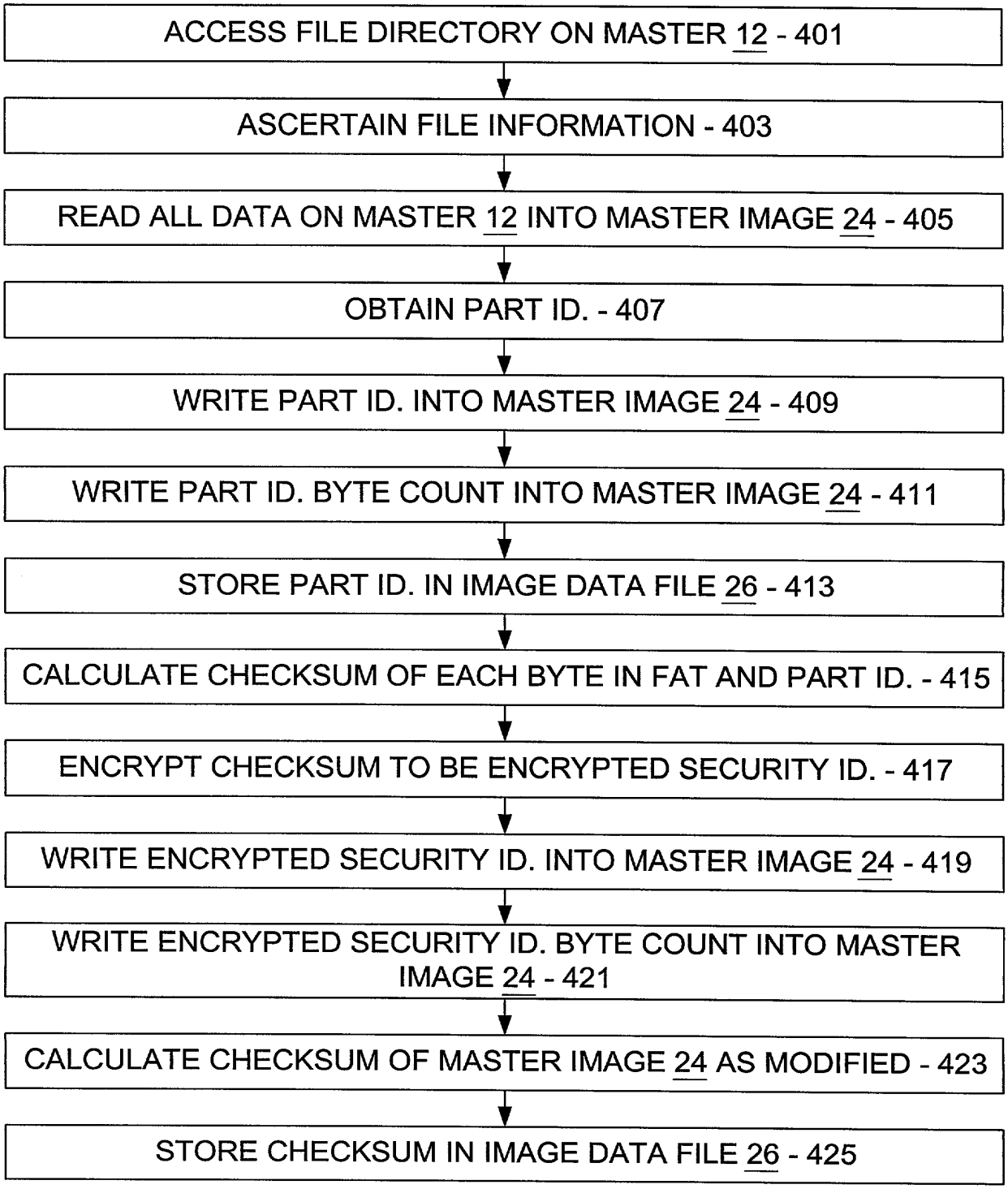
ACCESS FILE DIRECTORY ON MASTER 12 - 401
ASCERTAIN FILE INFORMATION - 403
READ ALL DATA ON MASTER 12 INTO MASTER IMAGE 24 - 405
OBTAIN PART ID. - 407
WRITE PART ID. INTO MASTER IMAGE 24 - 409
WRITE PART ID. BYTE COUNT INTO MASTER IMAGE 24 - 411
STORE PART ID. IN IMAGE DATA FILE 26 - 413
CALCULATE CHECKSUM OF EACH BYTE IN FAT AND PART ID. - 415
ENCRYPT CHECKSUM TO BE ENCRYPTED SECURITY ID. - 417
WRITE ENCRYPTED SECURITY ID. INTO MASTER IMAGE 24 - 419
WRITE ENCRYPTED SECURITY ID. BYTE COUNT INTO MASTER IMAGE 24 - 421
CALCULATE CHECKSUM OF MASTER IMAGE 24 AS MODIFIED - 423
STORE CHECKSUM IN IMAGE DATA FILE 26 - 425

FIG. 4

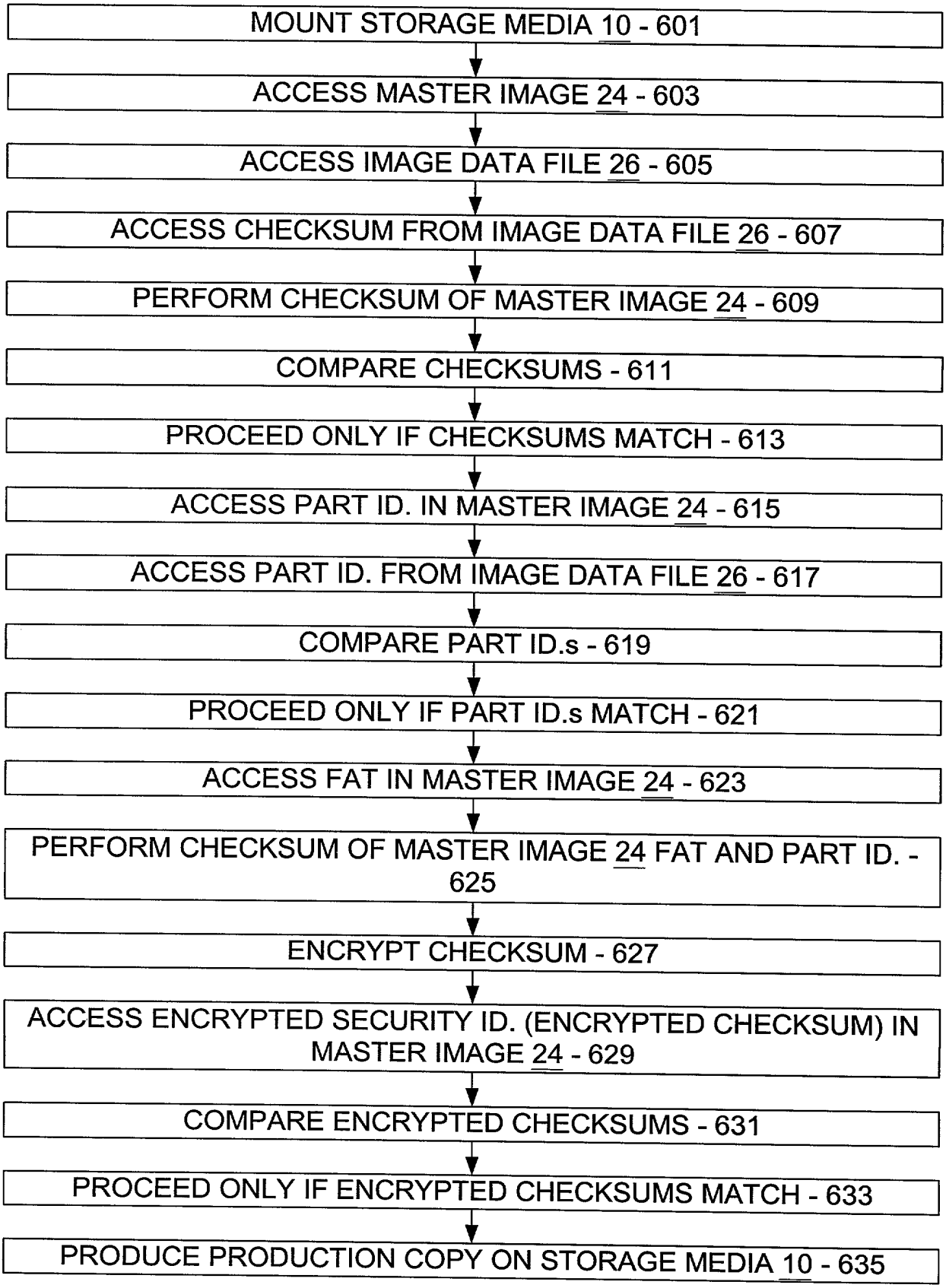
MOUNT STORAGE MEDIA 10 - 601
ACCESS MASTER IMAGE 24 - 603
ACCESS IMAGE DATA FILE 26 - 605
ACCESS CHECKSUM FROM IMAGE DATA FILE 26 - 607
PERFORM CHECKSUM OF MASTER IMAGE 24 - 609
COMPARE CHECKSUMS - 611
PROCEED ONLY IF CHECKSUMS MATCH - 613
ACCESS PART ID. IN MASTER IMAGE 24 - 615
ACCESS PART ID. FROM IMAGE DATA FILE 26 - 617
COMPARE PART ID.s - 619
PROCEED ONLY IF PART ID.s MATCH - 621
ACCESS FAT IN MASTER IMAGE 24 - 623
PERFORM CHECKSUM OF MASTER IMAGE 24 FAT AND PART ID. - 625
ENCRYPT CHECKSUM - 627
ACCESS ENCRYPTED SECURITY ID. (ENCRYPTED CHECKSUM) IN MASTER IMAGE 24 - 629
COMPARE ENCRYPTED CHECKSUMS - 631
PROCEED ONLY IF ENCRYPTED CHECKSUMS MATCH - 633
PRODUCE PRODUCTION COPY ON STORAGE MEDIA 10 - 635

FIG. 6

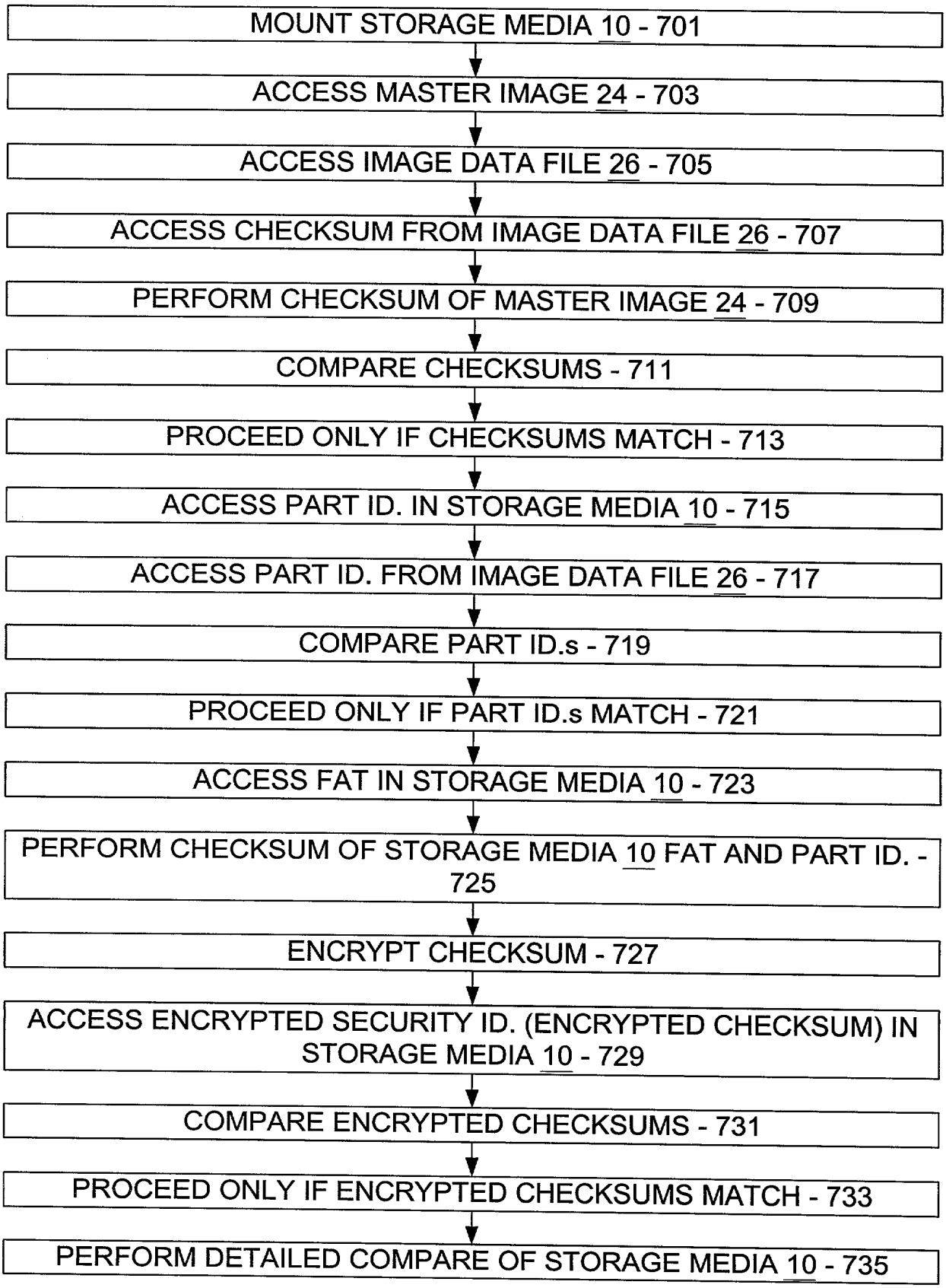
MOUNT STORAGE MEDIA 10 - 701
ACCESS MASTER IMAGE 24 - 703
ACCESS IMAGE DATA FILE 26 - 705
ACCESS CHECKSUM FROM IMAGE DATA FILE 26 - 707
PERFORM CHECKSUM OF MASTER IMAGE 24 - 709
COMPARE CHECKSUMS - 711
PROCEED ONLY IF CHECKSUMS MATCH - 713
ACCESS PART ID. IN STORAGE MEDIA 10 - 715
ACCESS PART ID. FROM IMAGE DATA FILE 26 - 717
COMPARE PART ID.s - 719
PROCEED ONLY IF PART ID.s MATCH - 721
ACCESS FAT IN STORAGE MEDIA 10 - 723
PERFORM CHECKSUM OF STORAGE MEDIA 10 FAT AND PART ID. - 725
ENCRYPT CHECKSUM - 727
ACCESS ENCRYPTED SECURITY ID. (ENCRYPTED CHECKSUM) IN STORAGE MEDIA 10 - 729
COMPARE ENCRYPTED CHECKSUMS - 731
PROCEED ONLY IF ENCRYPTED CHECKSUMS MATCH - 733
PERFORM DETAILED COMPARE OF STORAGE MEDIA 10 - 735

FIG. 7

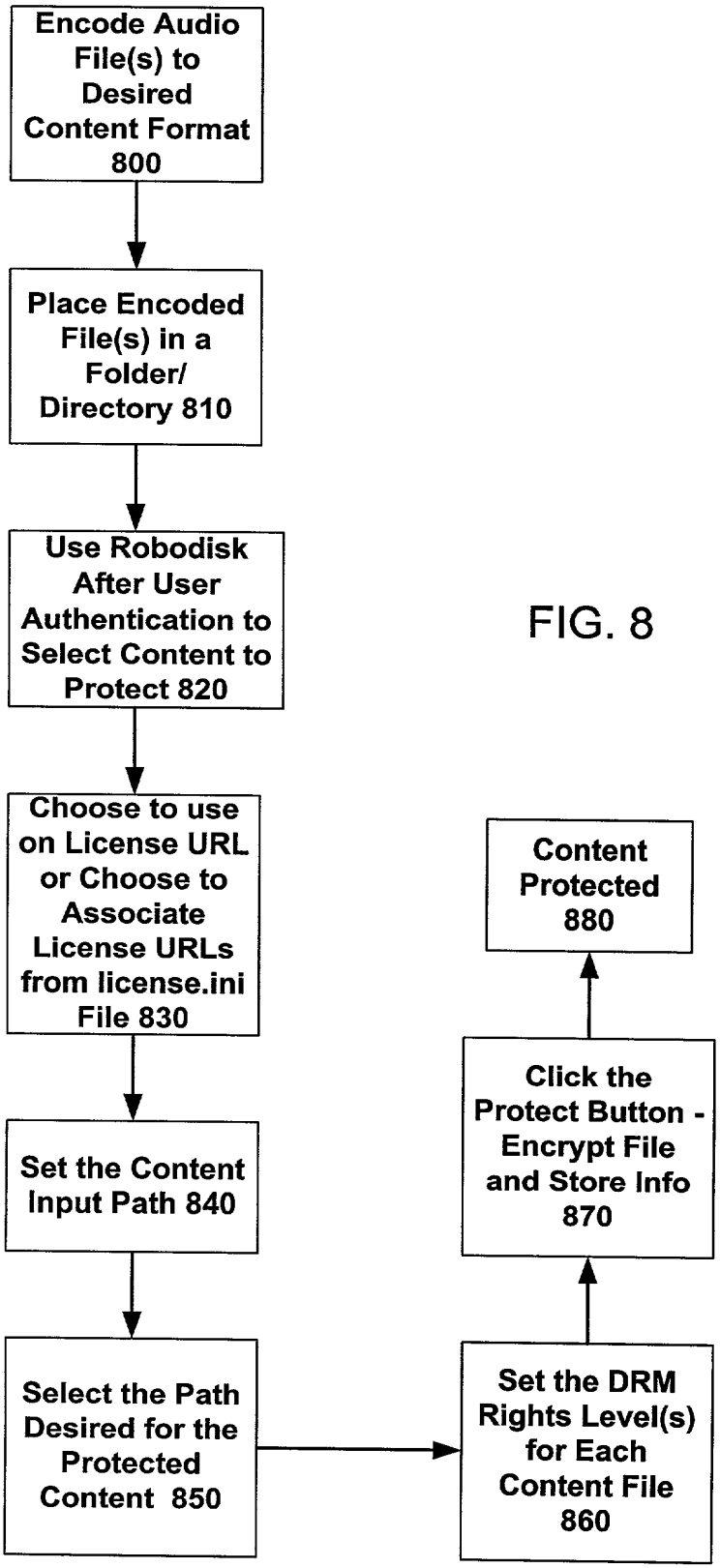
Encode Audio File(s) to Desired Content Format 800
Place Encoded File(s) in a Folder/ Directory 810
Use Robodisk After User Authentication to Select Content to Protect 820
Choose to use on License URL or Choose to Associate License URLs from license.ini File 830
Set the Content Input Path 840
Select the Path Desired for the Protected Content 850
Set the DRM Rights Level(s) for Each Content File 860
Click the Protect Button - Encrypt File and Store Info 870
Content Protected 880

FIG. 8

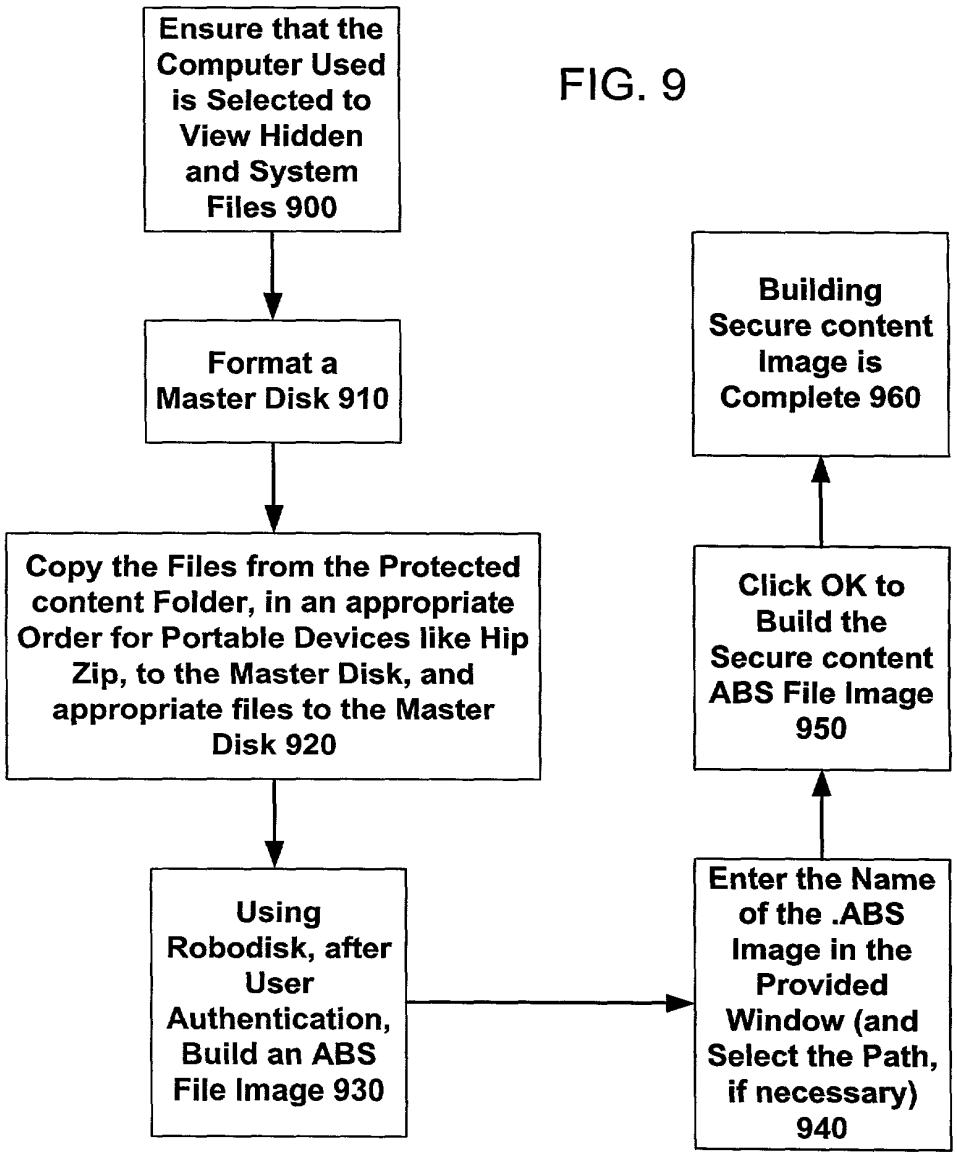
Ensure that the Computer Used is Selected to View Hidden and System Files 900
Format a Master Disk 910
Copy the Files from the Protected content Folder, in an appropriate Order for Portable Devices like Hip Zip, to the Master Disk, and appropriate files to the Master Disk 920
Using Robodisk, after User Authentication, Build an ABS File Image 930
Enter the Name of the .ABS Image in the Provided Window (and Select the Path, if necessary) 940
Click OK to Build the Secure content ABS File Image 950
Building Secure content Image is Complete 960

FIG. 9

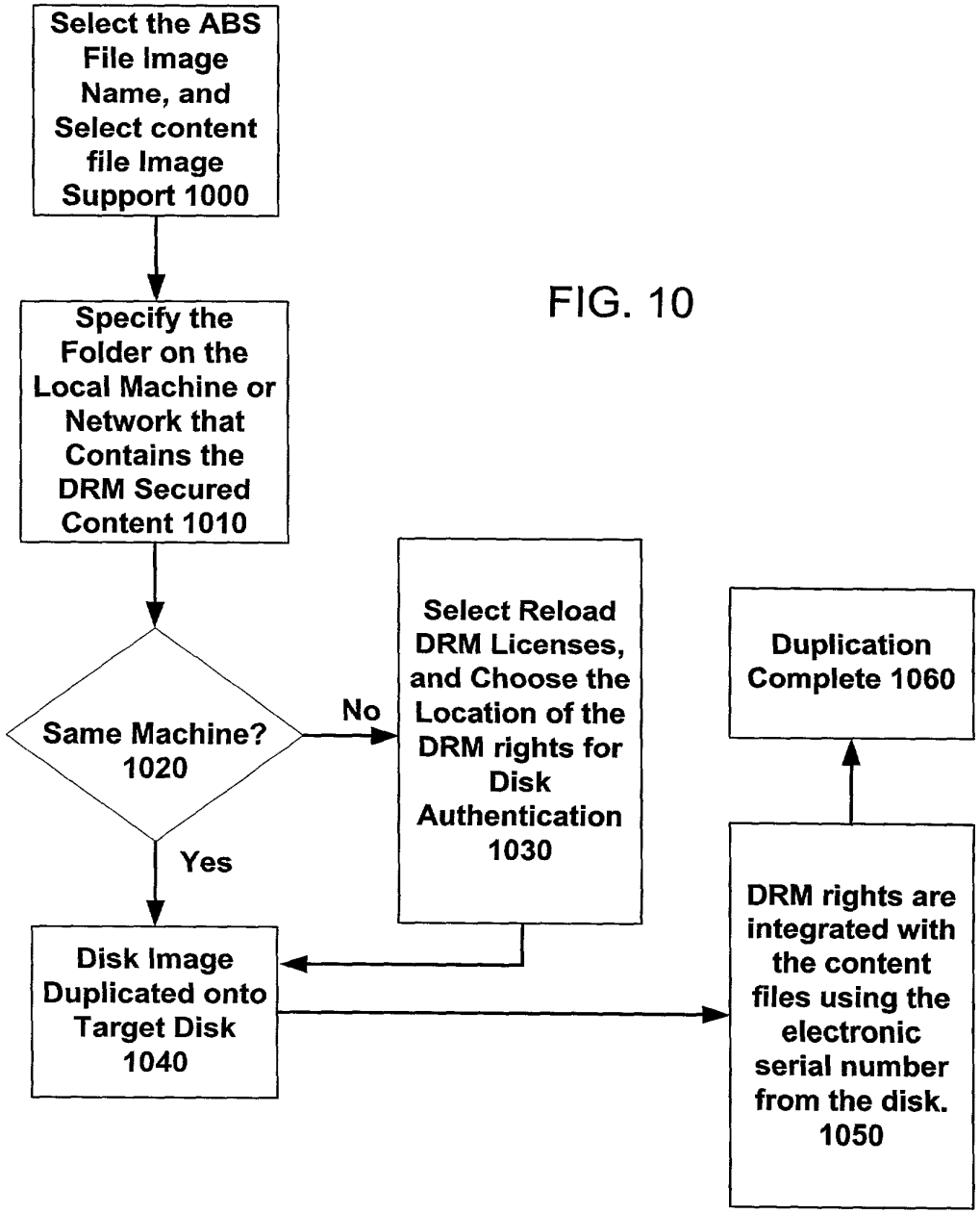
Select the ABS File Image Name, and Select content file Image Support 1000
Specify the Folder on the Local Machine or Network that Contains the DRM Secured Content 1010
Same Machine? 1020
No
Yes
Select Reload DRM Licenses, and Choose the Location of the DRM rights for Disk Authentication 1030
Disk Image Duplicated onto Target Disk 1040
DRM rights are integrated with the content files using the electronic serial number from the disk. 1050
Duplication Complete 1060

FIG. 10